Regras e Procedimentos de Deveres Básicos

ANBIMA

Sumário

INTRODUÇÃO

Estas Regras e Procedimentos de Deveres Básicos para as Instituições Participantes, aprovadas por todos os Fóruns de Representação de Mercados da ANBIMA, dispõem sobre as regras de Selos ANBIMA e as regras estruturais, quais sejam: (a) ambientes de controles; (b) segregação de atividades; (c) privacidade/proteção de dados pessoais; (d) plano de continuidade de negócios; (e) segurança da informação e (f) segurança cibernética.

Estas Regras e Procedimentos são consideradas transversais, visto que se aplicam a todos os Códigos ANBIMA e suas respectivas atividades. De modo a facilitar a consulta pelo mercado e evitar assimetria autorregulatória, incluímos estas regras e procedimentos em um único documento. As instituições participantes, ao aderirem aos Códigos ANBIMA, passam a aderir automaticamente à estas regras e procedimentos.

A ANBIMA, autorreguladora privada, tem competência para supervisionar apenas o disposto expressamente nestas regras e procedimentos, não estendendo, portanto, sua atuação às regras previstas nas normas regulamentares[1]. No decorrer deste documento fazemos referência ao termo "regulação" tão somente para fins educacionais e de modo não exaustivo, estritamente para que as instituições estejam cientes que além das regras de autorregulação aqui previstas há, adicionalmente, normas regulamentares a serem observadas em função de suas atividades.

[1] Tais como, Leis, Resoluções da Comissão de Valores Mobiliários e do Banco Central do Brasil.

TÍTULO I – DISPOSIÇÕES GERAIS

CAPÍTULO I – OBJETIVO E ABRANGÊNCIA

Art. 1º. O presente normativo tem por objetivo estabelecer as regras e os procedimentos para o uso dos Selos ANBIMA e para atendimento aos deveres básicos e à manutenção das estruturas internas mínimas que devem ser observadas por todas as instituições participantes que desempenham as atividades previstas nos Códigos ANBIMA.

§1º. As instituições participantes devem assegurar que este normativo seja também observado por todos os integrantes de seu grupo econômico que estejam autorizados, no Brasil, a desempenhar o exercício profissional das atividades referidas no caput.

§2º. A obrigação prevista no parágrafo acima não implica o reconhecimento, por parte das instituições participantes, da existência de qualquer modalidade de assunção, solidariedade ou transferência de responsabilidade entre estes integrantes, embora todas as referidas entidades estejam sujeitas aos princípios estabelecidos pelo presente normativo.

§3º. O disposto nessas Regras e Procedimentos não se aplica ao Código de Ofertas.

Art. 2º. As instituições participantes submetidas à ação reguladora e fiscalizadora do Conselho Monetário Nacional, do BC e da CVM, concordam, expressamente, que as atividades autorreguladas pelos Códigos ANBIMA excedem o limite de simples observância da regulação que lhes são aplicáveis, devendo, dessa forma, submeter-se também aos procedimentos estabelecidos por este normativo e pelos Códigos ANBIMA específicos de suas atividades.

Art. 3º. O presente normativo não se sobrepõe à regulação vigente e/ou aos Códigos ANBIMA, portanto, caso haja contradição entre as regras estabelecidas neste normativo e nos Códigos

ANBIMA e a regulação em vigor, a disposição contrária deste normativo deve ser desconsiderada, sem prejuízo das demais regras nele previstas.

Parágrafo único. Os deveres e responsabilidades atribuídos às instituições participantes que desempenham as atividades previstas nos Códigos ANBIMA se estendem, igualmente, em relação ao disposto nas regras e procedimentos aplicáveis a cada uma dessas atividades.

TÍTULO II – DEVERES BÁSICOS DAS INSTITUIÇÕES PARTICIPANTES

CAPÍTULO II – REGRAS ESTRUTURAIS

Art. 4º. O conteúdo dos documentos exigidos neste capítulo pode constar de um único documento, inclusive por grupo econômico, desde que haja clareza a respeito dos procedimentos e das regras exigidos em cada seção.

Parágrafo único. As instituições participantes devem revisar os documentos escritos exigidos por este capítulo, assim como as regras, os procedimentos, controles internos e monitoramentos em prazo não superior a 24 (vinte e quatro) meses ou em prazo inferior se exigido pela regulação, e, caso necessário, realizar a atualização.

Seção I – Ambientes de controles

Art. 5º. As instituições participantes devem possuir estruturas de controles internos e de compliance que sejam efetivas, consistentes e compatíveis com a sua natureza, o seu porte, a sua complexidade, o seu perfil de risco, o risco das operações realizadas e o seu modelo de negócio.

§1º. As estruturas de controles internos e de compliance de que trata o caput podem ser desempenhadas pelas instituições participantes em conjunto, na mesma estrutura, ou por unidades específicas.

§2º. A(s) área(s) a que se refere o parágrafo anterior deve(m):

I. ser independente(s) das áreas que possam limitar sua autonomia e autoridade para questionar os riscos assumidos nas operações realizadas pelas instituições participantes, observado o artigo 8º deste normativo;
II. ter livre acesso às informações necessárias para o exercício de suas atribuições;
III. ter colaboradores em quantidade suficiente, observado o disposto no caput, com experiência necessária para o exercício das atividades relacionadas à função de controles internos e compliance;
IV. definir as áreas e/ou os profissionais responsáveis por assegurar o cumprimento das obrigações previstas em cada seção e ter profissionais com a experiência necessária para o exercício das atividades relacionadas à função de controles internos e compliance, responsáveis por assegurar o cumprimento das obrigações previstas em cada seção, sem prejuízo do disposto no artigo 6º abaixo.
V. ter comunicação direta com a diretoria ou órgão equivalente, conforme aplicável, para relatar os resultados decorrentes das atividades relacionadas à função de controles internos e de compliance, incluindo possíveis irregularidades ou falhas identificadas.
VI. Conceder a seus colaboradores acesso regular à capacitação e conscientização sobre a atividades relacionadas à função de controles internos e compliance.

Art. 6º. As instituições participantes devem implementar e manter, em documento escrito, regras e procedimentos referentes as atividades de controles internos e de compliance que contenham, no mínimo:

I. o objetivo e o escopo da função de controles internos e de compliance;
II. o processo adotado para que as políticas e as demais regras internas relacionadas a controles internos e compliance sejam acessíveis a todos os profissionais de forma a assegurar que os procedimentos e as responsabilidades atribuídas aos diversos níveis da organização sejam conhecidos;

III. a divisão clara das responsabilidades dos profissionais envolvidos na função de controles internos e compliance da responsabilidade das demais áreas das instituições, de modo a evitar possíveis conflitos de interesses; e

IV. as medidas adotadas para garantir a independência e a adequada autoridade aos responsáveis pela função de controles internos e compliance nas instituições.

Art. 7º. As instituições participantes devem atribuir a responsabilidade pelos controles internos e pelo compliance a um diretor estatutário, sendo vedada a atuação em funções e atividades que possam gerar conflito de interesse.

Parágrafo único. As instituições participantes podem designar um único diretor responsável pelos controles internos e pelo compliance, ou podem indicar diretores específicos para cada função.

Seção II – Segregação de atividades

Art. 8º. O exercício das atividades dos Códigos ANBIMA deve ser segregado das demais atividades das instituições participantes e de seu grupo econômico que possam gerar conflitos de interesse.

§1º. Para o cumprimento do disposto no caput, as instituições participantes devem implementar e manter, em documento escrito, regras e procedimentos relativos à segregação das atividades que contenham, no mínimo:

I. Os processos adotados para segregação apropriada das funções atribuídas aos integrantes da instituição participante, de forma a evitar situações de conflito de interesses e mitigar a ocorrência de ilícitos legais ou contrários à regulação;

II. Quais áreas e atividades possuem a segregação funcional, logica e física, das áreas que desempenham as atividades dos Códigos ANBIMA de modo evitar conflitos de interesse; e

III. Como se dá o processo de identificação, controle e monitoramento das áreas identificadas como de potencial conflito de interesses.

Seção III – Privacidade e proteção de dados pessoais

Art. 9º. As instituições participantes devem implementar e manter atualizados, em documento escrito e com base em critérios próprios, regras e procedimentos que tratem da privacidade e dos dados pessoais a que as instituições participantes tenham acesso, incluindo, no mínimo:

I. Forma de atendimento a todos os princípios de diretrizes estabelecidas na LGPD;

II. Informação sobre o local em que a Política de Privacidade da instituição participante está disponível;

III. Descrição das metodologias, mecanismos e boas práticas de Segurança da Informação para seus funcionários, parceiros, terceiros e demais agentes participantes envolvidos, visando mitigar eventuais riscos de acesso indevido ou eventual vazamento de dados pessoais;

IV. Detalhamento do processo de Gestão de Riscos e Governança da instituição participante acerca do tema;

V. Como se dá o controle de privacidade e dados pessoais a que as instituições participantes tenham acesso, identificando, mas não se limitando a: controlador, operador, bases legais, finalidade, duração de tratamento, compartilhamento e responsabilidades;

VI. Critérios adotados para a proteção da integridade, confidencialidade e disponibilidade dos ativos de informação e dos dados pessoais tratados durante todo o seu ciclo de vida, conforme classificação da informação, abordando desde a geração até o descarte, incluindo armazenamento, acesso, tratamento, transmissão e transporte; e

VII. Regras aplicáveis aos profissionais para o gerenciamento de identidade e acesso aos ativos de informação e dados pessoais a que tenham acesso, desde o início até o término do relacionamento do profissional com as instituições participantes, inclusive nos casos de mudança de atividade dentro da mesma instituição participante, de forma a garantir o adequado tratamento dos dados.

Seção IV – Plano de continuidade de negócios

Art. 10. As instituições participantes devem implementar e manter, em documento escrito, plano de continuidade de negócios em que se observe, no mínimo:

I. Formas alternativas para processamento em situações de contingência, assegurando a continuidade das atividades em tempo hábil para cumprimento de suas responsabilidades;
II. Análise de riscos potenciais aos quais as instituições participantes estejam expostas com a indicação da medida de contingência a ser adotada para mitigação; e
III. Procedimentos de ativação, estabelecimento de prazos para a implementação e a designação das equipes que ficarão responsáveis pela operacionalização dos referidos planos.

Seção V – Segurança da Informação

Art. 11. As instituições participantes devem implementar e manter, em documento escrito, regras e procedimentos referentes a segurança da informação que contenham, no mínimo:

I. Quais são as informações consideradas, pelas instituições participantes, como confidenciais e privilegiadas;
II. Como se dá o processo de preservação das informações confidenciais e privilegiadas e quais área(s) e/ou profissional(is), incluindo os terceiros contratados, podem ter acesso a elas; e
III. Indicação se a instituição participante realiza testes do programa de segurança da informação, e em caso positivo, qual a periodicidade.
IV. Quais as ações de proteção, prevenção e controle para mitigar os riscos de vazamento de informações confidenciais e privilegiadas, a que instituição participante possa estar exposta;

V. Descrição dos mecanismos de controles e monitoramento para cada risco identificado, de forma a verificar sua efetividade e identificar eventuais incidentes; e

VI. Sem prejuízo da Seção IV deste capítulo (Plano de continuidade de negócios), a indicação de Plano de ação e de resposta a incidentes de segurança da informação, previstos durante a avaliação de riscos, garantindo a continuidade dos negócios ou a recuperação adequada em casos mais graves.

Art. 12. As instituições participantes devem exigir que seus profissionais e terceiros contratados assinem, de forma manual ou eletrônica, documento de confidencialidade sobre as informações confidenciais e privilegiadas que lhes tenham sido confiadas em virtude do exercício de suas atividades profissionais, excetuadas as hipóteses permitidas em lei.

§1º. As instituições participantes estão dispensadas de assinar o documento de que trata o caput caso o contrato de prestação de serviço do profissional ou do terceiro contratado tenha cláusula de confidencialidade.

§2º. Os terceiros, de que trata o caput, são os terceiros considerados pelas instituições participantes como relevantes e que em razão de suas atividades e funções precisam ter controle sobre as informações a que tenham acesso.

Seção VI – Segurança Cibernética

Art. 13. As instituições participantes devem implementar e manter, em documento escrito, regras e procedimentos referentes a segurança cibernética que contenham, no mínimo:

I. Identificação e avaliação de riscos, contendo:

   a. Quais os ativos considerados relevantes pelas instituições participantes, sejam eles equipamentos, sistemas, dados ou processos;

b. As vulnerabilidades internas ou externas em relação aos ativos previstos na alínea "a" acima;

c. Identificação da probabilidade de ocorrência e a magnitude dos impactos negativos, caso concretizadas as ameaças cibernéticas.

II. Quais as ações de proteção, prevenção e controle para mitigar os riscos de vazamento de informações confidenciais e privilegiadas e de ataques cibernéticos internos e externos a que instituição participante possa estar exposta;

III. Descrição dos mecanismos de controles e monitoramento para cada risco identificado, de forma a verificar sua efetividade e identificar eventuais incidentes; e

IV. Sem prejuízo da Seção IV deste capítulo (Plano de continuidade de negócios), a indicação de Plano de ação e de resposta que deve considerar os incidentes cibernéticos previstos durante a avaliação de riscos, garantindo a continuidade dos negócios ou a recuperação adequada em casos mais graves;

V. Indicação se a instituição participante realiza testes do programa de segurança cibernética, e em caso positivo, qual a periodicidade.

Parágrafo único. É recomendável que as instituições participantes observem, na elaboração do documento de que trata o caput, o guia ANBIMA de segurança cibernética disponível no site da Associação na internet.

Art. 14. Sem prejuízo das regras de contratação de terceiros previstas nos Códigos ANBIMA, as instituições participantes devem assegurar que suas regras e procedimentos de segurança cibernética contemplem a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, classificados como críticos e/ou de maior risco conforme a metodologia de cada instituição participante.

Parágrafo único. A contratação de serviços de processamento e armazenamento de dados de que trata o caput deve assegurar a verificação da capacidade do potencial prestador de serviço, incluindo, no mínimo:

I. O acesso das instituições participantes aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

II. A confidencialidade, a integridade, a disponibilidade e a recuperação das informações e dados processados ou armazenados pelo prestador de serviço;

III. A sua aderência a certificações exigidas pelas instituições participantes ou reguladores para a prestação do serviço a ser contratado, caso aplicável;

IV. O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

V. A identificação e a segregação dos dados dos clientes, funcionários, colaboradores ou terceiros relevantes das instituições participantes por meio de controles físicos ou lógicos;

VI. A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes, funcionários, colaboradores e terceiros relevantes das instituições participantes.

Seção VII – Regras gerais

Art. 15. As instituições participantes devem adotar e manter, em documento escrito, os mecanismos de acompanhamento com vistas a assegurar a implementação e a efetividade das regras, dos procedimentos e dos controles internos dispostos nas seções III, V e VI deste Capítulo, que devem conter, no que couber:

I. Quais processos e controles são adotados no acompanhamento de que trata o caput;

II. Definição de metodologias, métricas, critérios e indicadores adequados;

III. Identificação e a correção de eventuais deficiências.

Art. 16. Os instrumentos referidos no artigo anterior deverão incluir mecanismos de validação e testes, no mínimo, anuais, ou em prazo inferior se exigido pela regulação em vigor.

Parágrafo único. Os mecanismos de validação ou testes descritos têm como objetivo avaliar se as medidas de sigilo, proteção de dados e segurança cibernética são capazes de suportar, de modo satisfatório, os processos operacionais, sistemas e bancos de dados críticos, manter sua integridade, segurança e consistência na infraestrutura adotada e verificar se tais políticas ou planos podem ser ativados tempestivamente.

Art. 17. As instituições participantes deverão conceder acesso regular à capacitação e conscientização sobre práticas gerais de proteção de dados pessoais, segurança da informação e segurança cibernética, para todos os seus profissionais, incluindo terceiros.

Art. 18. Estas Regras e Procedimentos entram em vigor em [data].